Glossary

A

- **Authority:** Authority implies the right to exercise power in an organization.
- **Authentication:** Authentication is the process of identifying genuine users by verifying the credentials provided for accessing the resources.
- **Authorization:** Authorization is the process of allocating specific resources to users based on their respective privileges.
- **App:** App refers to the software program that allows clients and users to sign in onto cloud to access, store, and exchange data.
- **Activity Report:** Activity report includes all the activities that the testing team had performed across the organization and can also include various documents to support the claims.

B

- **Black-box Testing**: Black-box testing, also known as behavioral testing, refers to the process in which the tester has no prior knowledge or information about a system.
- **Blind Testing:** A blind-testing process focuses on and simulates the methodologies of a real attacker.
- **Black-box Assessment:** In black-box assessment, no background information is given to the testing analyst. They need to spend a large amount of time in researching the environment and organization.
- **Black-Box Social Engineering Penetration Testing:** In black-box social engineering penetration testing, also called a trial-and-error approach, the client does not provide any information about the target to the tester.
- **Baiting:** Baiting is a technique in which pen testers tempt the target user with something alluring in exchange for important information such as login details and other sensitive data.
- **Buffer Overflow:** A buffer overflow involves overriding the crucial registry portions and modifying internal variables with random values to control the execution of the process or to crash it completely.
- **Bots:** Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks, such as web spidering and search engine indexing.
- **Botnet:** A botnet is a huge network of the compromised systems and can be used to launch DOS attacks.
- **BGP:** Border Gateway Protocol (BGP) is an external routing protocol which is used to communicate between different autonomous systems.
- **BACnet:** BACnet is a standard data communication protocol for building automation and control networks.
- **Binary Coding:** Each instruction is associated with a binary code that will be directly interpreted by the processor during program execution (the machine code).
- **Block Started by Symbol (BSS) segment:** This segment stores uninitialized static/global variables and will be filled with zeros by the operating system (OS).

C

- **Crowdsourced Penetration Testing Service**: Crowdsourced penetration testing service is an open-ended pen testing assignment in which pen testers worldwide attempt to determine the vulnerabilities in a target environment.
- **Consensus/Social Proof:** Consensus or social proof refers to the fact that people usually like or do things that other people like or do.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Covert Channel:** Covert channel can be defined as a hidden communication mechanism through the established security infrastructure.
- **Configuration Management:** Configuration management is the process of handling changes made to the servers and systems used to access the application, databases, and other connected devices to maintain integrity.
- **Cryptography:** Cryptography is the process of keeping the user information secured by using proper encryption techniques.
- **Cross-site Scripting (XSS):** Cross-site scripting (XSS) is a vulnerability in dynamically generated webpages that enable malicious attackers to inject client-side script into webpages viewed by other users.
- **CRLF Injection Attack:** In the CRLF injection attack, the attackers split the HTTP responses and inserts customized CRLF characters into the headers to generate custom response from the target web application.
- **Connection String:** The connection string is a set of parameters defining the connection process of a web application with the database.
- **Connection Pool DoS:** An attacker examines the connection pooling settings of the application, constructs a large malicious SQL query, and runs multiple queries simultaneously to consume all connections in the connection pool, causing database queries to fail for legitimate users.
- **Control-plane Protocols:** These protocols Include all engineering activities, i.e., reprogramming of the controller, upload/download of the firmware, etc.
- **Cloud Pen Testing:** Cloud pen testing refers to evaluation of security across virtual machines, installed apps, and operating systems in a cloud.
- **Cloud Web Security Scanner:** Cloud web security scanner identifies vulnerabilities such as cross site scripting and outdated libraries during development before they enter into production.
- **Cloud Anomaly Detection:** Cloud anomaly detection utilizes behavioral signals to detect security abnormalities like unusual activity and leaked credentials in virtual machines or GCP projects.
- **Client-side Test Report:** Client-side test report includes the details of the client-side test such as phishing, spear-phishing, spam, and social engineering attacks used during the testing.

D

- **Double-blind Testing:** Double-blind testing involves the testing of the organization's security monitoring, incident identification, and response procedures.
- **Data Use Agreement:** A data use agreement (DUA) governs the disclosure and use of data in the nationwide databases of the Healthcare Cost and Utilization Project (HCUP) of the US Department of Health & Human Services.
- **DNS Interrogation:** DNS interrogation is the process of collecting information about the DNS servers and the corresponding DNS records of a target organization.
- **Dumpster Diving:** Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins.
- **DNS Server:** A DNS server is a database that contains information about all the IP addresses and their respective hostnames.
- **DNS Poisoning:** Using a DNS poisoning attack, you can inject fake records into the cache of a DNS server, corrupt the DNS tables, and redirects a victim to the malicious IP address.
- **Database Fingerprinting:** Database fingerprinting is to determine the database name, type of database, version, users, output mechanism, user privilege level, and OS interaction level by various methods.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Dynamic Testing:** In this type of testing, pen tester should perform activities like fuzzing, traffic interception and analysis, injection in order to check the thick client against injection attacks.
- **DoS Attack:** DoS attack is a type of attack in which the services are reduced or made unavailable to the valid user.
- **Data Modification Attack:** The Data Modification attack is a more dangerous attack that not only captures and stores target's data exchange but also modifies it using a radio frequency device.
- **Data Corruption Attack:** Data corruption attack is a type of DoS attack, where the third-party attempts to corrupt the data being transmitted between the two endpoints.
- **Data-plane Protocols: These** protocols are used to pass parameters and registers between human–machine interface (HMI) SCADA applications and I/O.
- **Data Segment:** This segment stores static/global variables initialized by the programmer.
- **Draft Report:** A draft report refers to the rough copy of a report before finalizing the process flow.
- **Document Properties:** Document properties refer to the description of the document being submitted to the target organization.

E

- **Engagement Letter:** The EL (Engagement Letter) is a document authorizing the penetration testing provider to conduct an engagement for the testing organization.
- **Email Harvesting:** Email harvesting is a process in which a large number of email addresses are obtained through different methods.
- **Eavesdropping:** Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages.
- **Elicitation:** Elicitation is the technique of extracting information from the victim by drawing them into normal and disarming conversations.
- **External Network Penetration Testing:** External network penetration testing is the method of assessing the assets and identifying vulnerabilities that could help the attackers to exploit the network from outside.
- **External Vulnerability Assessment:** External vulnerability assessment refers to the process of identifying vulnerabilities in externally accessible devices, OSs, and applications of an organization.
- **Enumeration:** Enumeration is the process of extracting usernames, machine names, network resources, shares, IP tables, routing tables, SNMP and DNS details, and services from a system or network.
- **EIGRP:** Enhanced Interior Gateway Routing Protocol (EIGRP) is a proprietary routing protocol of Cisco systems.
- **Exceptions:** Exceptions are events that require special processing or additional resources to execute the inputs.
- **Event Threat Detection:** Event threat detection monitors the organization's Cloud Logging stream and collects logs from one or multiple projects to detect security breaches such as presence of malware, brute force SSH attempts, and cryptomining.
- **Evans Debugger:** The Evans debugger (EDB) is a graphical user interface (GUI)-based debugger capable of performing static and dynamic analysis of binaries, similar to GDB.
- **Executive Report:** Executive report is a short briefing of the complete testing process and includes details of the tested components, vulnerabilities, misconfigurations, updates required, and other details that can help the authorities make decisions for securing the target.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Executive Summary:** The executive summary provides a high-level view of the test goals and results in the form of both risks and business impact in a simple and understandable way.

F

- **Familiarity/Likeness:** Familiarity or likeness implies the fact that people are more likely to get persuaded to do something when asked by someone they like.
- **Fragmentation Scanning:** Fragmentation scanning is the process of sending the entire packet by dividing it into a set of IP fragments.
- **Fingerprinting:** Fingerprinting refers to the process of finding the OS or services running on a device placed on the target network.
- **Firewall:** A firewall is a software- or hardware-based system located at the network gateway that protects the resources of a private network from users on other networks.
- **Fuzz Testing:** Fuzz testing, also called Fuzzing, is a form of Black Box testing in which the testers use automated tools to perform the injection attacks to find any implementation bugs in an app.
- **Frame Injection:** Frame injection attack involves injecting the frames in scripts, where an application does not validate the input.

G

- **Gray-box Penetration Testing:** In gray-box penetration testing, security assessment and testing are internally performed; the process of testing examines the scope of access by insiders within the organization's network.
- **Gray-box Assessment:** In Gray-box assessment, some information is given to the analyst to assist in their research.
- **Get-Out-of-Jail-Free Card:** A get-out-of-jail-free card is an element that helps a person or organization emerge from an undesirable situation.
- **Google's Advanced Operators:** Google's advanced operators can be used to refine a search and create complex queries to find, filter, and sort specific information regarding the target.
- **Greed:** Greed implies that some people are possessive in nature and wish to acquire huge amounts of wealth from doing illegal activities.
- **GNU Project Debugger:** The GNU Project debugger (GDB) allows the observation of activity "inside" another program while it executes or at the moment it crashed.

H

- **Hping:** Hping is a TCP ping utility that allows you to pass through a firewall even if they are blocked.
- **HMI/controller machine:** Usually, a Windows workstation is used as the master to manage and control PLCs on the network through client software.
- **Heap:** The heap is used to provide space for dynamic memory allocation and is managed by function calls such as malloc, calloc, realloc, and free.
- **Host Report:** Host report provides information about the hosts tested, vulnerabilities found, exploited hosts, etc.

I

- **In-house penetration testing service:** In in-house penetration testing penetration testing service model, organizations have a dedicated penetration testing team in place, which is continuously engaged in in-house pen testing assignments.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Intimidation:** Intimidation refers to an attempt that is made to frighten a victim into taking several actions by using bullying tactics.
- **Internal Penetration Testing:** Internal penetration testing refers to the analysis performed inside the organization and provides the complete picture of the security of an organization.
- **Insecure Cryptographic Storage:** Insecure cryptographic storage refers to use of weak encryption codes and algorithms to encrypt the web application data while storing it in the database.
- **Internet of Things (IoT):** IoT is referred as the network of computing devices that are web-enabled and have the capability of sensing, collecting, and sending data using sensors, communication hardware, and processors that are embedded within the device.
- **Infrastructure as a Service (IaaS):** CSP controls the hardware, network, storage, servers, and virtualization part of cloud while the client will control the operating systems, services, data, and apps on cloud.

J

- **Jammers:** Jammers (jamming devices) are used to block the wireless network communication within the specific area.

K

- **Kerberos:** Kerberos is an authentication protocol which allows the nodes in a network to communicate with each other in a secured way by providing their identity to the other nodes.

L

- **Latency:** Latency is considered as the time delay that takes place before any operation is performed or transfer of data begins.
- **Lock-in Problem:** Lock-in" refers to a situation in which a subscriber cannot switch to another CSP.
- **Letter of Attestation:** Letter of Attestation is a statement or declaration taken from an independent third party that lends credibility to the penetration test performed on the client organization.

M

- **Media Dropping**: Media dropping technique involves the dropping of a USB flash drive near a parking lot or entrance area where people can easily see it.
- **Mission Briefing:** Mission briefing refers to the process of providing detailed information about the penetration test, scope, and goal to the team responsible for performing the tests.
- **Metagoofil:** Metagoofil is an information-gathering tool designed for extracting the metadata of public documents (PDF, doc, xls, ppt, docx, pptx, and xlsx) belonging to a target company.
- **MAC Flooding:** MAC flooding is a computer network enumeration and footprinting technique (attack) that involves the spoofing of a network interface's unique MAC address.
- **MAC Spoofing:** MAC spoofing is a technique of manipulating or masking the MAC address of any network device with a random MAC address.
- **Multistage Processes:** Multistage processes involve a defined sequence of requests; attempt to submit these requests out of the expected sequence
- **Modbus:** Modbus is an application-layer messaging protocol positioned at level 7 of the Open Systems Interconnection (OSI) model.
- **Modbus RTU:** Modbus RTU is a serial communication protocol that connects different devices on the same network, enabling communication between them.
- **Modbus TCP/IP:** Modbus TCP/IP covers the use of Modbus communication via an "Intranet" or "Internet" environment using TCP/IP protocols.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **MAC Filtering:** MAC filtering is a process used by network administrator to allow only the list of approved MAC addresses to connect to a router in the wireless network.
- **MITM (Man-in-the-Middle) Attack:** A MITM attack is an active internet attack in which the hacker attempts to intercept, read, or alter information between two computers.
- **Malicious Insiders:** Malicious insiders are disgruntled current/former employees, contractors, or other business partners who have/had authorized access to cloud resources and could intentionally exceed or misuse that access to compromise the confidentiality, integrity, or availability of the company's information.

N

- **Network Penetration Testing:** Network penetration testing is a well-known method for identifying vulnerabilities in networks, systems, hosts, and network devices before attackers recognize and exploit them.
- **National Institute of Standards and Technology:** The National Institute of Standards and Technology (NIST) is a federal technology agency that works with the industry to develop and apply technology, measurements, and standards.
- **Network Time Protocol (NTP):** The Network Time Protocol (NTP) is an internet protocol used for synchronizing time across the computer networks and is enabled by default.
- **Narrative Reports:** Narrative reports contain an in-depth description of the technical aspects of the report.
- **Near Field Communication (NFC):** Near Field Communication (NFC) is a short-range, wireless connection standard that uses radio waves to establish communication between electronic devices.

O

- **Open Web Application Security Project**: The Open Web Application Security Project is an open-source methodology. It provides a set of tools and a knowledge base, which help in protecting web applications and services.
- **Off-site Testing:** Off-site testing involves testing employees' security awareness during their daily activities.
- **On-site Testing:** On-site testing involves testing the physical security of an organization and the security policies in place.

P

- **Penetration Testing:** Penetration testing is a type of security testing that evaluates an organization's ability to protect its infrastructure such as network, applications, systems, and users against external as well as internal threats.
- **Penetration Testing as a Service (PTaaS):** It is a cloud service that provides penetration testing along with the resources needed to conduct at-a-point-in-time and continuous penetration tests.
- **Pretexting**: In pretexting technique, the hacker calls the target person and asks for information while pretending to be an authentic user that needs assistance. By performing this technique, the penetration tester can target nontechnical users who may disclose sensitive data.
- **Policy Penetration Tester:** A policy penetration tester determines whether all the policies developed and analyzed are up to date and check for their implementation across the organization.
- **Points-of-Contact:** A POC (Points-of-Contact) refers to the identification and means of communication with person(s) and organizations(s) associated with resource(s).
- **Phishing Frenzy:** Phishing Frenzy is an open-source Ruby on Rails application that is leveraged by penetration testers to manage email phishing campaigns.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Phishing:** Phishing is a technique in which the pen tester sends an email or provides a link that falsely claims to be from a legitimate site in an attempt to acquire a user's personal or account information.
- **Piggybacking:** Piggybacking usually implies entry into the building or security area with the consent of an authorized person who is not aware of the pen tester's identity.
- **Port Scanning:** Port scanning is the process of sending a message to all the ports of a system to check whether they are open or closed.
- **Port Forwarding:** Redirect connection for a port on the first victim to another host.
- **Packet Injection:** Packet injection, also known as forging packets or spoofing packets, is the process of developing fake packets and inserting them into an established network.
- **Power Analysis Attack:** Power analysis is the type of side channel attack that enables you to crack passwords by analyzing power consumption patterns of a network device.
- **Polymorphic Shellcode:** Polymorphic shellcode is a shellcode that contains hidden malicious code in an encrypted form.
- **Patch:** Patch is a piece of code used as temporary fixes for software vulnerabilities.
- **PLC:** A PLC is a physical system connected with a power supply and the capability to communicate over Ethernet networks.
- **Packet Injection:** Packet injection, also known as forging packets or spoofing packets, is the process of developing fake packets and inserting them into an established network.
- **Platform as a Service (PaaS):** In PaaS, the client will be responsible for the data stored on cloud and apps running on it while the CSP will be controlling all the other resources.
- **Python Exploit Development Assistance:** Python Exploit Development Assistance (PEDA) for GDB can enhance the display of GDB by colorizing and displaying disassembly codes, registers, and memory information during debugging.
- **Penetration Testing Report:** The penetration testing report is a structured report that details the findings of the penetration tests that are conducted for a client.

R

- **ROI for a Penetration Testing:** ROI for a pen test is demonstrated with the help of a business case scenario, which includes the expenditure and involved profits.
- **Rules of Engagement:** The rules of engagement (ROE) is the formal permission to conduct penetration testing.
- **Red-Team-Oriented Penetration Testing Approach:** Red-team-oriented penetration testing approach is an adversarial goal-based assessment in which the pen tester must mimic a real attacker and target an environment.
- **Request for Proposal:** An RFP (Request for Proposal) is an invitation to penetration testers to submit their proposals of penetration testing services to the client organization.
- **Reverse Social Engineering:** In reverse social engineering, the pen tester assumes the role of a person in authority so that employees ask them for information.
- **Remote procedure call (RPC):** Remote procedure call (RPC) is a protocol that is used by a computer to communicate or request any other computer in the network without having to understand the network's details.
- **Rootkit:** A rootkit is a set of programs that any attacker uses to penetrate a system.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Recommendations:** Recommendations refer to the suggestions that a tester provides the organization based on the analysis of test reports for mitigating vulnerabilities and strengthening the organization's security level.
- **Radio Frequency Identification (RFID):** RFID is a technology that uses radio signals to identify and record the presence of objects.
- **RFID Penetration Testing:** RFID penetration testing helps the tester to perform vulnerability assessment on RFID systems and identify various possible threats to the target organization.
- **RFID Cloning:** RFID cloning involves capturing the data from a legitimate RFID tag, and then creates a clone of it using a new chip.
- **Replay Attack:** Replay attack is a process of consuming the computing resources of the tags by repeating/delaying a valid data transmission of the network.
- **Recommendations:** Recommendations refer to the suggestions that a tester provides the organization based on the analysis of test reports for mitigating vulnerabilities and strengthening the organization's security level.

S

- **Security Audit**: A security audit checks whether an organization follows a set of standard security policies and procedures.
- **Social Engineering Penetration Testing:** Social engineering penetration testing is intended to test the employees' compliance with the security policies and practices predefined by the management.
- **Social Engineering:** Social engineering is one of the most attempted malicious activities that attackers use to gain access to the sensitive data of an individual or an organization.
- **Scope Creeping:** Scope creeping is the process of adding new services or objectives to a project that has already been defined.
- **Shodan:** Shodan is a search engine for finding specific devices and device types that exist online and are open on the Internet.
- **SMiShing:** In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number.
- **Shoulder Surfing:** Shoulder surfing is the technique of observing or looking over someone's shoulder as they key in information into a device.
- **System Administrator:** A system administrator in an organization is responsible for maintaining the IT systems, and they may thus have critical information such as the type and version of operating system and admin passwords that could be helpful for a pen tester in planning an attack.
- **Session initiation protocol (SIP):** Session initiation protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
- **SSH:** SSH (secure shell) is a protocol for establishing secured communication between different computers in an unsecured network.
- **Sniffing:** Sniffing is a process of monitoring and capturing all data packets passing through a network.
- **Source Routing:** Source routing is a method where the sender specifies a path that a packet should take in order to travel in a network.
- **Session:** Session refers to a sequence of request and response transactions between a user and a web application.
- **Session Splicing:** Session splicing is an IDS evasion technique that exploits how some IDSs do not reconstruct sessions before performing pattern matching on the data.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Sitemap:** Sitemap refers to a file that holds a list of webpages related to a website.
- **Session Fixation:** Session fixation is an attack technique that forces a user's session ID to an explicit value.
- **System Testing:** System testing refers to the process of performing penetration tests of the system to determine the test if any of its vulnerabilities would result in compromise of thick client application running on it.
- **Static Testing:** Static testing refers to the process of examining the installation files of a thick-client to identify any malicious code, erroneous processes in decompilation and encryption, and check the integrity of the code.
- **Software as a Service (SaaS):** In SaaS, CSP will be controlling all the resources except for the data stored on cloud and may perform complete pen test of cloud.
- **Security Health Analytics:** Security Health Analytics assesses the overall security state and activity of virtual machines, containers, network, storage, and identity and access management policies.
- **Stack:** The stack is used for storing local variables defined inside functions, as well as data related to function calls such as the return address and arguments.
- **Scope of the Project:** Scope of the project refers to the total number of IP addresses, apps, devices, hosts, and other network resources that the organization had listed in the contract.
- **Summary of Evaluation:** The summary of evaluation refers to the detailed reports of the evaluations performed along with a description of all the processes.
- **Summary of Findings:** The summary of findings contains information about the discoveries the testers made during the test, including the risks and threats of all the target devices.
- **Sign-off Document:** The sign-off document refers to a written end-of-contract letter that both parties are advised to sign after the completion of the penetration testing process.

T

- **Tailgating:** Tailgating implies accessing a building or secured area without the consent of the authorized person.
- **Telephony Security Assessment:** Telephony security assessment checks the security issues of voice technologies used in organizations.
- **Test Plan:** A test plan is a document that details the structure of procedures for a penetration test.
- **Tailgating:** Tailgating implies access to a building or secured area without the consent of an authorized person.
- **Telnet:** Telnet is a client–server network protocol used on the Internet or local area networks, which provides the sign-in sessions for a user on the Internet.
- **Throughput:** Throughput is considered as the maximum rate at which the data is transferred in a channel.
- **Thick Clients:** The thick clients refer to the applications installed and run on the client-side systems.
- **Text segment:** This block of memory stores the executable code of the program and is usually read-only.
- **Testing Methodology:** In penetration testing, methodology refers to a standard framework process that the testers are advised to follow to perform the testing.

U

- **Urgency:** Urgency implies encouraging people to take an immediate action.
- **Username Enumeration:** The username enumeration is the process of identifying different usernames, which users had assigned to access the web application.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **URL Encoding:** URL encoding converts unsafe ASCII characters into a format that can be transmitted over the Internet.
- **URL Parameter Tampering:** A web parameter tampering attack involves the manipulation of input parameters that a user can enter through the URL in the web application in order to modify application data, such as user credentials and permissions, price, and quantity of products.
- **User Report:** This report includes the information of users who were identified and targeted during the testing process along with the tasks performed by them.

V

- **Vulnerability Assessment:** Vulnerability assessment is a process of identifying vulnerabilities or loopholes in any organizational network infrastructure.
- **Vishing:** Vishing (voice phishing or Voice over IP (VoIP) phishing) is an impersonation technique in which the pen tester uses VoIP technology to trick individuals into revealing their critical financial and personal information.
- **Virtual Network Computing (VNC):** Virtual network computing (VNC) is a graphical desktop sharing system that uses the remote frame buffer protocol to remotely control another computer.
- **Vulnerability Report:** Vulnerability report provides detailed information about all the vulnerabilities found during the pen testing process.
- **Version History:** Version history refers to a record of all the version control tracked changes made on the report, including the names of the people who made the revisions, date and time when they made the changes, and a description of the changes made.

W

- **White-box Penetration Testing:** White-box testing is also known as structural testing. In this type of testing, the tester is provided with various information of the organization before the start of the test.
- **White-box Assessment:** In white-box assessment, the analyst is given all the information required to penetrate the organization's environment.
- **Web Application Penetration Testing:** Web application penetration testing helps in detecting security issues in web applications due to insecure design and development practices.
- **Wireless Network Penetration Testing:** Wireless penetration testing is the process of actively evaluating information security measures in a wireless network.
- **Waiver:** A waiver is the voluntary relinquishment or surrender of some known right or privilege by an organization.
- **Web Spidering:** Web spidering or web crawling is the process of finding all the web pages related to a website or a web application.
- **Web Shell:** Malicious script used by an attacker with the intent to escalate and maintain persistent access on an already compromised web application.
- **Web Parameter Tampering Attack:** A web parameter tampering attack involves the manipulation of input parameters that a user can enter through the URL in the web application in order to modify application data, such as user credentials and permissions, price, and quantity of products.
- **Web Services XML Poisoning:** Hackers insert malicious XML code in SOAP requests to perform XML node manipulation or XML schema poisoning to generate errors in XML parsing logic and break execution logic.
- **WS Replay:** In this attack, the attackers intercept a message and replay it to impersonate the original sender.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Well-structured Reports:** Well-structured reports contain a high-level representation of the test results in the form of charts and graphs.
- **Wireless Network (Wi-Fi):** Wireless Network (Wi-Fi) refers to wireless local area networks (WLAN) based on IEEE 802.11 standard where it allows the device to access the network from anywhere within range of an access point (AP).
- **Wired Equivalent Privacy (WEP):** Wired Equivalent Privacy (WEP) is a security algorithm for 802.11 wireless networks that provides data confidentiality in wireless networks.

X

- **XPath Injection Attack:** XPath Injection is an attack technique used to exploit websites that construct XPath queries from user-supplied input.

Certified Penetration Testing Professional Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.